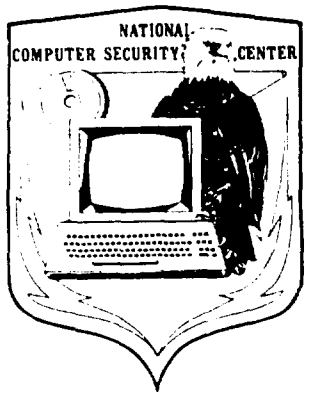
CSC-EPL-87/005

(2)



NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF PIKE CREEK COMPUTER COMPANY SGT SECURITY

VERSION 4A

16 July 1987

SUB-SYSTEM EVALUATION REPORT

PIKE CREEK COMPUTER COMPANY

SGT SECURITY VERSION 4A

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

July 15, 1987

CSC-EPL-87/005
Library No. S228,517

This page intentionally left blank.

CSC-EPL-87/005
Library No. S228,517

FOREWORD

This publication, the Sub-system Evaluation Report, Pike Creek Computer Company, SGT SECURITY version 4A, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of an evaluation of Pike Creek's SGT SECURITY version 4A product. The requirements stated in this report are taken from DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, dated December 1985.

Approved:

July 15, 1987

Eliot Sohmer
Chief, Product Evaluations and Technical Guidelines
National Computer Security Center

ACKNOWLEDGEMENTS

Evaluation Team Members

Joseph Bulger

William Geer

John W. Taylor

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

CONTENTS

		Page
	Foreword	iii
	Acknowledgements	iv
	Executive Summary	vii
Section 1	Introduction	1
	Background	1
	The NCSC Computer Security Sub-system Evaluation Program	1
Section 2	Product Evaluation	3
	Product Overview	3
	Evaluation of Functionality	3
	Evaluation of Documentation	4
Section 3	The Product in a Trusted Environment	5
Section 4	Product Testing	7
Section 5	Evaluators' Comments	9

This page intentionally left blank.

EXECUTIVE SUMMARY

The SGT SECURITY product has been evaluated by the National Computer Security Center (NCSC). SGT SECURITY is considered to be a security sub system, rather than a complete trusted computer system, therefore it was evaluated against the relevant subset of the security requirements in the DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, dated December 1985. The subset for this product includes object reuse. Additionally, SGT SECURITY was evaluated against the overwrite procedures outlined in the DEPARTMENT OF DEFENSE MAGNETIC REMANENCE SECURITY GUIDELINE (Guideline), dated 15 November 1985.

The NCSC evaluation team has determined that SGT SECURITY, version 4A, when invoked, applies the requirement of object reuse for magnetic media and random-access memory, and applies the overwrite procedures, as specified in the Guideline, to data stored on internal magnetic media of an IBM PC/XT or PC/AT running PC-DOS(1). SGT SECURITY is manually invoked to provide these features, and therefore the Site Security Officer (SSO) must assure that the product is used.

Since the product is used on a single-state microprocessor, the system administrator must take certain precautions in protecting the code, operating system, and microcomputer from unauthorized modification or destruction. With these precautions, SGT SECURITY may be used to clear internal magnetic media for reuse within the same security level or to perform overwrite steps which may be defined as part of a SSO's declassification procedure. The actual procedures to be followed to declassify magnetic media must still be established by the SSO's organization. SGT SECURITY may be used on all data except where an established security policy specifies a different procedure.

Overall, this product provides effective protection against data scavenging (recovery of deleted material). The product, when invoked, overwrites all data and files stored in internal magnetic media. SGT SECURITY may be a useful adjunct to security by itself, and if integrated within a complete security policy may be helpful to a SSO.

---

(1) IBM PC/XT, PC/AT and PC-DOS are registered trademarks of International Business Machines Corporation.

This page intentionally left blank.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all Federal Government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

Tne primary goal of the NCSC is to encourage the widespread availability of trusted computer systems: systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Sub systems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub system evaluation is limited to consideration of the sub system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub system's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

SGT SECURITY is a microcomputer software package which operates on an IBM PC, PC XT, PC AT or BIOS compatible under MS-DOS(1) or PC-DOS. The product provides an erasure mechanism for the internal magnetic media and random-access memory. The erasure mechanism may be used as a command-line driven security supplement to DOS, or through the product user interface. The user interface is a single screen containing menu selections to perform the erasure function.

The SGT SECURITY product is composed of a program command file and ten program routines. The interface is command driven and has a variety of options available. These options are divided by SGT SECURITY into modes and commands. The modes define the scope of the files displayed, the number of default overwrite cycles, whether the memory is to be cleared, and the video mode. The command options select the disk on which the operations are to be performed, and which files are to be erased, including the entire disk. The commands and typing conventions used by the program are common throughout the program and are reasonably standard.

Evaluation of Functionality

Object Reuse

After invoking SGT SECURITY in the mode desired, the product provides an effective manually invoked erasure feature for internal magnetic media and the random access memory (RAM) installed on the microcomputer system. Erasure of the RAM installed in the microcomputer is done using the DOS memory management conventions. Specifically, the product does not clear RAM that has been designated as the storage space for a Terminate, Stay Resident (TSR) routine. SGT SECURITY clears the memory above this pointer up to the start of PC-DOS's reserved memory.

---

(1) MS-DOS is a registered trademark of Microsoft Corporation.

Magnetic Remanence Guideline Procedure

The DEPARTMENT OF DEFENSE MAGNETIC REMANENCE SECURITY GUIDELINE recommends procedures that may be used to ensure the erasure of magnetic media. SGT SECURITY provides an effective means for overwriting all addressable locations on the internal magnetic media in a manner which conforms to the procedures.

Evaluation of Documentation

The SGT SECURITY software package provides two manuals, the User Manual, and the Security Officer Manual, which together describe the system.

The User Manual is intended for the general user. This manual provides the information needed for daily operation of SGT SECURITY. The manual includes the proper procedures for erasure of microcomputer internal magnetic media, and random access memory.

The Security Officer Manual is for the Site Security Officer. This document is designed to instruct the security officer on the administration of the SGT SECURITY system. The manual includes information on the security features and management utilities necessary to operate the system.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to data created with these systems. Initially, protection was provided solely by the individuals who maintained physical possession of their own data and operating system on a floppy disk, giving a reasonably high assurance of maintaining data and code integrity. These procedural controls isolated users, and thus prevented intentional or accidental access to other users' data. Other security mechanisms were not deemed necessary since users were only able to inflict damage on their own data, or copy of the operating system.

The advent of inexpensive and reliable hard disk drives introduced new security implications. In today's working environment, it is common to have many users share and store their data on the hard disk of a shared microcomputer. In this environment, users no longer have the assurance that their data is protected from unauthorized access, or even that the underlying operating system has not been corrupted. Procedural controls can no longer provide adequate user isolation and the controlled sharing necessary for this environment.

SGT SECURITY can provide added security to this environment by assuring the user that data erased with SGT SECURITY is not retrievable with standard disk utilities. The security mechanism can be maintained only if both the operating system in which SGT SECURITY executes and SGT SECURITY's code are protected from unauthorized modification. SGT SECURITY operates on a single state hardware machine, and as such the non-privileged user operates in the same memory space in which the security-related system functions. As a result, SGT SECURITY is at risk and care must be taken to ensure that it has not been modified.

This page intentionally left blank.

PRODUCT TESTING

Testing represents a significant portion of a sub-system evaluation. The functional test suite focused on the erasure feature provided by the Pike Creek Computer Company's SGT SECURITY product. Testing was intended as a functional checklist to ensure that SGT SECURITY's erasure mechanism functioned as documented. The team's testing of the erasure mechanism involved attempts to locate flaws, but did not attempt to subvert the operation of the program.

Modification of the source code was done to show that each of the functions worked in the manner described in the manual. All functions of the product were tested and found to perform in the manner documented and expected. Independently, the object code was disassembled and checked against the source code. Additionally, during testing the program was halted at various spots and operations verified through the use of utilities. All checks revealed nominal operation. The testing uncovered no flaws in design or implementation.

This page intentionally left blank.

EVALUATORS' COMMENTS

The SGT SECURITY product may be useful in a number of areas where the control of sensitive data is concerned. The product provides a useful feature to the user concerned about ensuring the erasure of information from the microcomputer. The procedures that Pike Creek Computer Company has incorporated into their product show thought and understanding of the issues involved.

SGT SECURITY adheres to the magnetic media erasure procedures outlined in the DEPARTMENT OF DEFENSE MAGNETIC REMANENCE SECURITY GUIDELINE (Guideline). The procedures are considered sufficient to handle the erasure of magnetic media. A Site Security Officer (SSO) could use the product in defining an overall policy to address the issues of data remanence. The actual procedures to be followed to declassify magnetic media must still be established by the SSO's organization.

The SSO must ensure that the correct program is distributed to users. The concern over ensuring that a correct program is distributed is due to the fact that the executable code could be modified by a utility such as DOS' DEBUG. The modified program could then no longer be trusted to perform as designed. For this reason, use of the SGT SECURITY program should be restricted to trusted personel. Ideally, verification of SGT SECURITY's integrity should be assured each time that sensitive data is required to be overwritten or cleared.

Pike Creek Computer Company has provided a method to alleviate the problem of ensuring that a correct version of the program has been distributed to users. Pike Creek Computer Company provides SGT INSPECTOR to address this problem. SGT INSPECTOR is a program that may be used to validate that a working copy of SGT SECURITY is correct. SGT INSPECTOR was provided to us by the vendor, but is not part of the evaluated configuration.

Overall, the evaluation team feels that this product may be used as an useful adjunct to security, and may be helpful to security officers trying to dispose of sensitive data.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS NONE
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT DISTRIBUTION UNLIMITED
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-87/005	5 MONITORING ORGANIZATION REPORT NUMBER(S) S228,517
6a NAME OF PERFORMING ORGANIZATION National Computer Security Center 6b OFFICE SYMBOL (If applicable) C12	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State, and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000	7b ADDRESS (City, State, and ZIP Code)
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)

(U) Sub-system Evaluation Report, Pike Creek Computer Co. SGT SECURITY, Version 4A

12 PERSONAL AUTHOR(S)
Joseph Bulger, William Geer, John Taylor

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Final	FROM _____ TO _____	870715	18

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	
			SGT SECURITY, Pike Creek Computer Co., NCSC, TCSEC, sub-system, Magnetic Remanence Security Guideline, Object Reuse, (AT)

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The Pike Creek Computer Company's SGT SECURITY product was evaluated against the Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985.

The product is a software package which, when properly invoked, provides protection against data scavenging. This report documents the evaluation of this product.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL LTC Lloyd D. Gary, USA	22b TELEPHONE (Include Area Code) (301) 859-4458 22c OFFICE SYMBOL C/C12

DD Form 1473, JUN 86 Previous editions are obsolete SECURITY CLASSIFICATION OF THIS PAGE